What is claimed is:

1   1.   A method for a capacity planning server in a packet network to calculate
2   access router to access router traffic matrixes by using ingress and egress files
3   derived from flow records, each ingress file comprising a plurality of ingress
4   records in which each ingress record represents an incoming flow, each egress file
5   comprising a plurality of egress records in which each egress record represents an
6   outgoing flow, the method comprising the steps of:
7   identifying ingress and egress records in the ingress and egress files that
8   match; and
9   calculating a traffic matrix using the matched ingress and egress records.

1   2.   The method of claim 1 wherein the step of calculating a traffic matrix
2   further comprises the step of creating a hash set for each egress file.

1   3.   The method of claim 2 wherein the step of calculating a traffic matrix
2   further comprises the step of creating a key value by concatenating source
3   addresses and destination addresses from an egress record.

1   4.   The method of claim 3 wherein the step of calculating a traffic matrix
2   further comprises the step of adding the key value to the hash set.

1   5.   The method of claim 4 wherein the step of calculating a traffic matrix
2   further comprises the step of creating a key value by concatenating source
3   addresses and destination addresses from an ingress record.

1   6.   The method of claim 5 wherein the step of calculating a traffic matrix
2   further comprises the step of performing a test to determine if the key value for an
3   ingress record exists in a hash set for an egress file.

1 7.   The method of claim 6 wherein the step of calculating a traffic matrix
2 further comprises the step of annotating an ingress record with indexes of egress
3 routers for a flow record.

1 8.   The method of claim 7 wherein the step of calculating a traffic matrix
2 further comprises the step of incrementing an egress router count in the ingress
3 record when the ingress record is annotated.

1 9.   The method of claim 8 wherein the step of calculating a traffic matrix
2 further comprises the step of searching the hash set for every egress file for the
3 key value for every ingress record.

1 10.   The method of claim 9 wherein the step of calculating a traffic matrix
2 further comprises the step of calculating the traffic matrix elements by processing
3 the annotated ingress records.

1 11.   The method of claim 10 wherein the step of calculating a traffic matrix
2 further comprises the step of identifying specific elements in a traffic matrix using
3 data from an annotated ingress record.

1 12.   The method of claim 11 wherein the step of calculating a traffic matrix
2 further comprises the step of identifying specific elements by ingress router index,
3 egress router indexes, and type-of-service.

1 13.   The method of claim 12 wherein the step of calculating a traffic matrix
2 further comprises the step of adding byte and packet counts from an annotated
3 ingress record to the traffic matrix elements.

1 14.   The method of claim 1 wherein the traffic matrices are calculated using
2 non-sampled flow records.

1   15.   The method of claim 14 wherein the traffic matrices are calculated for a

2   virtual private network.

1   16.   The method of claim 1 wherein the traffic matrices are calculated using

2   sampled flow records.

1   17.   The method of claim 16 wherein the traffic matrix is calculated for a

2   virtual private network.

1   18.   The method of claim 16 further comprising the steps of:

2   using data from the traffic matrix to compute a distribution matrix;

3   post-processing the traffic matrix; and

4   outputting the traffic matrix.

1   19.   The method of claim 18 wherein the step of post-processing the traffic

2   matrix further comprises the step of determining the total bytes and packets for

3   each row of the traffic matrix.

1   20.   The method of claim 19 wherein the step of post-processing the traffic

2   matrix further comprises the step of dividing the bytes and packets for each entry

3   in the traffic matrix by the totals computed for that row.

1   21.   The method of claim 20 wherein the step of post-processing the traffic

2   matrix further comprises the step of determining the unmatched ingress records

3   for each row of the traffic matrix.

1   22.   The method of claim 21 wherein the step of post-processing the traffic

2   matrix further comprises the step of assigning the unmatched ingress records to all

3   potential egress routers in the same percentages computed for the distribution

4   matrix.

1 23.   A method for a capacity planning server in a packet network to calculate

2 service node to service node traffic matrixes by using ingress and egress files

3 derived from flow records, each ingress file comprising a plurality of ingress

4 records in which each ingress record represents an incoming flow, each egress file

5 comprising a plurality of egress records in which each egress record represents an

6 outgoing flow, the method comprising the steps of:

7   identifying ingress and egress records in the ingress and egress files that

8 match; and

9   calculating a traffic matrix using the matched ingress and egress records.

1 24.   The method of claim 23 wherein the step of calculating a traffic matrix

2 further comprises the step of creating a hash set for each egress file.

1 25.   The method of claim 24 wherein the step of calculating a traffic matrix

2 further comprises the step of creating a key value by concatenating source

3 addresses and destination addresses from an egress record.

1 26.   The method of claim 25 wherein the step of calculating a traffic matrix

2 further comprises the step of adding the key value to the hash set.

1 27.   The method of claim 26 wherein the step of calculating a traffic matrix

2 further comprises the step of creating a key value by concatenating source

3 addresses and destination addresses from an ingress record.

1 28.   The method of claim 27 wherein the step of calculating a traffic matrix

2 further comprises the step of performing a test to determine if the key value for an

3 ingress record exists in a hash set for an egress file.

1 29.   The method of claim 28 wherein the step of calculating a traffic matrix

2 further comprises the step of annotating an ingress record with indexes of egress

3 routers for a flow record.

1　30.　The method of claim 29 wherein the step of calculating a traffic matrix

2　further comprises the step of incrementing an egress router count in the ingress

3　record when the ingress record is annotated.

1　31.　The method of claim 30 wherein the step of calculating a traffic matrix

2　further comprises the step of searching the hash set for every egress file for the

3　key value for every ingress record.

1　32.　The method of claim 31 wherein the step of calculating a traffic matrix

2　further comprises the step of calculating the traffic matrix elements by processing

3　the annotated ingress records.

1　33.　The method of claim 32 wherein the step of calculating a traffic matrix

2　further comprises the step of identifying specific elements in a traffic matrix using

3　data from an annotated ingress record and a configuration file.

1　34.　The method of claim 33 wherein the step of calculating a traffic matrix

2　further comprises the step of mapping an access router name to a service node

3　index.

1　35.　The method of claim 34 wherein the step of calculating a traffic matrix

2　further comprises the step of identifying the traffic matrix elements by ingress

3　service node index, egress service node indexes, and type-of-service.

1　36.　The method of claim 35 wherein the step of calculating a traffic matrix

2　further comprises the step of adding byte and packet counts from an annotated

3　ingress record to the traffic matrix elements.

1　37.　The method of claim 23 wherein the traffic matrices are calculated using

2　non-sampled flow records.

1   38.   The method of claim 37 wherein the traffic matrices are calculated for a

2   virtual private network.

1   39.   The method of claim 23 wherein the traffic matrices are calculated using

2   sampled flow records.

1   40.   The method of claim 39 wherein the traffic matrix is calculated for a

2   virtual private network.

1   41.   The method of claim 39 further comprising the steps of:

2   using data from the traffic matrix to compute a distribution matrix;

3   post-processing the traffic matrix; and

4   outputting the traffic matrix.

1   42.   The method of claim 41 wherein the step of post-processing the traffic

2   matrix further comprises the step of determining the total bytes and packets for

3   each row of the traffic matrix.

1   43.   The method of claim 42 wherein the step of post-processing the traffic

2   matrix further comprises the step of dividing the bytes and packets for each entry

3   in the traffic matrix by the totals computed for that row.

1   44.   The method of claim 43 wherein the step of post-processing the traffic

2   matrix further comprises the step of determining the unmatched ingress records

3   for each row of the traffic matrix.

1   45.   The method of claim 44 wherein the step of post-processing the traffic

2   matrix further comprises the step of assigning the unmatched ingress records to all

3   potential egress routers in the same percentages computed for the distribution

4   matrix.